Certified Installation and Configuration for the Cisco Secure PIX Firewall Version 5.2(3)

January 2001

Contents

This document describes how to install and configure a PIX 515, PIX 520, or PIX 525 for use with Cisco Secure PIX Firewall software version 5.2(3) as certified by Common Criteria Evaluation Assurance Level 4 (EAL4).

Note Any changes to the information provided in this document will invalidate the certified Cisco Secure PIX Firewall and may make it insecure.

This document includes the following sections:

Corporate Headquarters: Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

This document is an addendum to the Cisco Secure PIX Firewall Version 5.2 documentation set, which should be read prior to use of the Cisco Secure PIX Firewall. This document provides references to the following Cisco Secure PIX Firewall documentation:

- *Installation Guide for the Cisco Secure PIX Firewall Version 5.2*
- *Configuration Guide for the Cisco Secure PIX Firewall Version 5.2*
- *Regulatory Compliance and Safety Information for the Cisco Secure PIX Firewall Version 5.2*
- *System Log Messages for the Cisco Secure PIX Firewall Version 5.2*
- *Release Notes for the Cisco Secure PIX Firewall Version 5.2(1)*
- *Release Notes for the Cisco Secure PIX Firewall Version 5.2(2)*
- *Release Notes for the Cisco Secure PIX Firewall Version 5.2(3)*

This document provides information on the installation and configuration of the Common Criteria Certified Cisco Secure PIX Firewall.

Note The *IPSec User Guide for the Cisco Secure PIX Firewall Version 5.2* is not referenced in this document because the information in that document *does not* form part of the Common Criteria Certified Cisco Secure PIX Firewall Version 5.2(3).

PIX Firewall documentation is available online at the following site:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/index.htm.

Audience

This document is written for administrators configuring a Common Criteria Certified Cisco Secure PIX Firewall version 5.2(3) using a PIX 515, PIX 520, or PIX 525. This document assumes you are familiar with networks and network terminology, that you are a trusted individual, and that you have been trained for use with the Internet and its associated terms and applications.

Security Information

In addition to the *Regulatory Compliance and Safety Information for the Cisco Secure PIX Firewall Version 5.2*, the sections that follow provide additional security information for use with a Common Criteria Certified Cisco Secure PIX Firewall.

Security Policy

Ensure that your PIX Firewall is delivered, installed, managed, and operated in a manner that maintains a security policy. The *Configuration Guide for the Cisco Secure PIX Firewall Version 5.2* provides guidance on how to define a security policy.

Security Implementation Considerations

The sections that follow provide implementation considerations that need to be addressed to administer the PIX Firewall in a secure manner.

Certified Configuration

Only version 5.2(3) can be used to ensure a secure configuration. Changing the PIX Firewall software to a different version invalidates the secure configuration. The PIX Firewall must also be configured as the only network connection between the networks connected to the firewall's interfaces.

The following hardware and software features are outside the scope of the defined Target of Evaluation (TOE) Security Functions. These have not been evaluated and do not form part of the certified product configuration. The certified Cisco Secure PIX Firewall version 5.2(3) does not include the use of the following:

- Cut-Through Proxies
- Failover
- Network Address Translation (NAT)
- Routing Information Protocol (RIP)
- Remote Management
- Simple Network Management Protocol (SNMP)
- Dynamic Host Configuration Protocol (DHCP) Server
- Virtual Private Networks (VPNs)
- Authentication, authorization, and accounting (AAA) server to provide identification and authentication
- Accepting updates for internal data structures (for example, routing tables) from an authorized host

The configuration of the PIX Firewall should be reviewed on a regular basis to ensure that the configuration continues to meet the organization's security objectives (as defined in the security policy) in the face of the following:

- Changes in the Cisco Secure PIX Firewall configuration
- Changes in the security objectives
- Changes in the threats presented by the external network
- Changes in the internal hosts and services available to the external network by the internal network

Physical Security

The PIX Firewall must only be administered at the PIX Firewall console from a locked room to which only the administrator has access.

Access Control

You must set the enable mode password using the **enable password** command. A good password has a combination of alphabetic and numeric characters as well as punctuation characters. This password must be at least eight characters long. We recommend that you tell the password to someone who is in a position of trust. If you lose the password, you must contact customer support to gain access to your unit.

Servers and Proxies

To ensure complete security when the PIX Firewall is shipped, inbound access to all proxies and servers is initially disabled. After the installation, you must explicitly permit each service and enable the ones necessary for your security policy. Refer to the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.2* and this document for information on how to configure the PIX Firewall. Certification requires a completely controlled environment in which specified services are allowed and all others denied.

Log Files and Messages

Log files are kept for all connection requests and server activity. Monitoring activity in the log files is an important aspect of your network security and should be conducted regularly. Monitoring the log files lets you take appropriate and timely action when you detect breaches of security or events that are likely to lead to a security breach in the future. Use the **logging** command to view log files messages. Refer to the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.2* and this document for information on logging, messaging, and archiving.

Trusted and Untrusted Networks

The PIX Firewall can be used to isolate your network from the Internet or from another network. Trusted networks are usually your internal network and untrusted networks may be the Internet or any other network. Therefore, the PIX Firewall must be configured so that it acts as the only network connection between your internal network and any external networks. The PIX Firewall will deny any information flows for which no rule is defined.

Your security implementation is based on the control of traffic from one network to the other, and should support your security policy.

Access Lists

The **access-list** command operates on a first match basis. Therefore, the last rule added to the access list is the last rule checked. The administrator should make a note of the last rule during initial configuration, because it may impact the remainder of the rule parsing.

Public Access Servers

If you are planning to host public access servers, you must decide where they will be located in relation to the PIX Firewall. Placing servers on the network outside the PIX Firewall leaves them open to attack. Placing servers on the internal network means you must allow access through the PIX Firewall to the servers.

Using FTP

File Transfer Protocol (FTP) is used to retrieve or deposit files on a remote system. Allowing users to access internal FTP servers directly leaves many opportunities for abuse. This service should be of concern when designing your security policy. The functionality provided by the TFTP configuration server is outside the scope of the certified Target of Evaluation (TOE).

Monitoring and Maintenance

The PIX Firewall provides several ways to monitor the firewall, from logs to messages.

- Ensure you know how you will monitor the PIX Firewall, both for performance and for possible security issues.
- Plan your backups. If there should be a hardware or software problem, you may need to restore the PIX Firewall configuration.
- The configuration of the PIX Firewall should be reviewed on a regular basis to ensure that the configuration meets the organization’s security objectives in the face of the following:
  - Changes in the PIX Firewall configuration
  - Changes in the security objectives
  - Changes in the threats presented by the external network
  - Changes in the internal hosts and services available to the external network by the internal network

Auditing Component Requirements

The PIX Firewall interacts with a Windows NT system for the purpose of storing the audit data. The auditing machine requirements are a Pentium II or later PC running Windows NT 4.0 with Service Pack 4 and Y2K patches.

Note We recommend that you use a certified version of the Windows NT Server for the machine holding the audit records.

The auditing machine will provide suitable audit records to the administrator, protect the stored audit records from unauthorized deletion, and detect modifications to the audit records. It is the responsibility of the administrator to regularly review the audit records provided by the PIX Firewall and take any relevant action as necessary to ensure the security of the PIX Firewall.

The location of the auditing machine and records should only be accessible to the administrator.

Determining the Software Version

Use the **show version** command to verify the software version of your PIX Firewall unit.

Installation Notes

The following sections in the *Installation Guide for Cisco Secure PIX Firewall Version 5.2* are supported on a certified PIX Firewall and should be followed when installing the certified PIX Firewall:

- Introduction, including safety recommendations, maintaining safety with electricity, and general site requirements in Chapter 1, "Introduction"
- Installation Overview and Installing a PIX 515, PIX 520, and PIX 525 models and Hardware and Software requirements for version 5.2 in Chapter 2, "Installing a PIX Firewall"
- Installing the PIX Firewall Syslog Server (PFSS) in Chapter 4, "Installing the PIX Firewall Syslog Server (PFSS)"
- Opening a PIX Firewall Chassis for PIX 515, PIX 520, and PIX 525 models in Chapter 5, "Opening a PIX Firewall Chassis"
- Installing a Memory Upgrade for PIX 515, PIX 520, and PIX 525 models in Chapter 6, "Installing a Memory Upgrade"
- Installing a Circuit Board for PIX 515, PIX 520, and PIX 525 models in Chapter 7, "Installing a Circuit Board"
- Installing a DC Voltage PIX 515 and PIX 520 in Chapter 8, "Installing a DC Voltage PIX 515 or PIX 520"

The following sections in the *Installation Guide for Cisco Secure PIX Firewall Version 5.2* are not supported on the certified configuration of the PIX Firewall. The features covered by these sections are outside the scope of the evaluated PIX Firewall and should not be installed:

- Installing Failover in Chapter 3, "Installing Failover"
- Installing a Private Link VPN board in Chapter 7, "Installing a Circuit Board"
- Installing the PIX Firewall Setup Wizard in Chapter 9, "Installing the PIX Firewall Setup Wizard"

Verification of Image

To verify that the PIX Firewall has not been tampered with during delivery, execute the following procedures:

Once the PIX Firewall has been unpacked, complete the 56-bit key form to obtain an activation key, from the following Cisco website:

http:www.cisco.com/kobayashi/sw-center/internet/pix-56bit-license-request.shtml

You need the following information to complete the form:

- Serial number
- Customer e-mail address
- Export acknowledgement

Once the form is submitted, the activation key will be sent by e-mail directly back to the customer e-mail address.

Once the activation key has been received, the PIX Firewall should be started up in accordance with the *Installation Guide for the Cisco Secure PIX Firewall Version 5.2*, Chapter 2.

At the prompt, type the **show version** command.

The activation key is displayed in four parts. The activation key displayed should be verified against the downloaded activation key.

Additional Notes

1. Do not attempt to load version 5.2(3) on a PIX Firewall unit containing less than 32 MB of memory. While the PIX Firewall may appear to permit this configuration, upon reboot, the PIX Firewall unit will continuously fail. You can stop the failure loop by immediately inserting a previous version diskette into the PIX Firewall unit and then pressing the reboot switch. This note only applies to PIX Firewall units with a diskette drive, not to the PIX 515 or PIX 525.
2. After installing additional memory in a PIX 520, do not remove the memory strips after you install them and have powered on the unit, or the PIX Firewall unit will become inoperable.
3. A PIX Firewall unit containing a 16-MB Flash memory card cannot be downgraded to version 4.4(1), 4.4(2), 5.0(1), or 5.0(2).
4. Version 5.1 on a PIX 515 cannot be downgraded to previous version 4.4(1) images.

Configuration Notes

The following features of the PIX 515, PIX 520, and PIX 525 version 5.2(3) as stated in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.2* are included in the certified configuration of the PIX Firewall:

- Everything as stated in Chapter 1, “Introduction,” except those features listed in this document that are not supported. Read this document carefully and consider the Security Policy section of this document.
- PIX 515 configuration with the exceptions noted.
- Everything else except for what is stated as not supported in this document.

The following features of the PIX 515, PIX 520, and PIX 525 version 5.2(3) as stated in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.2* are *not* supported in the certified configuration of the PIX Firewall:

- Chapter 1, “Introduction,” PIX Firewall features including:
  - AAA Service Selection
  - AAA Server Groups
  - Boothelper Installation
  - Cut-Through Proxies
  - Failover
  - FTP and URL logging
  - PIX Firewall Manager
  - IPSec
  - Java Filtering
  - Mail Guard
  - PPTP

  - Setup Wizard
  - Telnet Interface
  - TFTP Configuration Server
  - FTP Image Downloading
  - URL Filtering
  - VPN
- The following Chapter 2, “Configuring the PIX Firewall,” sections are not supported in a certified PIX Firewall:
  - Upgrading from a Previous Version, Steps 1 and 2
  - Step 2—Get the Most Current Software section on downloading the image using TFTP
  - Step 3—Configure Network Routing sections on Setting a Windows 95 and Windows 98 Default Route or a MacOS Default Route
  - Step 12—Add Telnet Console Access
  - Step 16—Viewing Messages from a Telnet Console Session
  - Step 17—Add AAA User Authentication
- Chapter 3, “Advanced Configurations”
- Chapter 4, “Configuration Examples”
- Chapter 5, “Command Reference,” features listed in the “Certified Configuration” section of this document

Disabling NAT

NAT must not be included in the configured certified PIX Firewall. By default, the PIX Firewall assumes NAT is configured.

NAT must be disabled. To disable NAT, the following steps are required:

1. Configure an **access-list** command statement that matches any IP traffic.
2. Associate the NAT access list to all interfaces to enable the certified environment to bypass the NAT processing.

Disabling Example

The following example lists the command statements for a certified PIX Firewall with the three interfaces inside, outside, and intf2:

```
access-list no-nat-list permit ip any any
nat (inside) 0 access-list no-nat-list
nat (outside) 0 access-list no-nat-list
nat (intf2) 0 access-list no-nat-list
```

Disabling NAT Warning

Through the use of the disabling NAT commands, the administrator initiates the capability to let users on the higher security interface access a lower security interface. Therefore, at this stage all traffic from the internal network will be allowed out, until a single rule (irrespective of its content) has been bound to the higher interface, thereby invoking the default deny all rule at the end of the access list bound to the interface.

Use of the **clear nat** command does not return the NAT settings to the default when the product has just been loaded. In this instance, the product will be left permitting connections from a higher security interface to the lower security interface, therefore affecting security. It is therefore recommended that the **clear nat** command not be used to remove the **nat 0 0** disable Network Address Translation setting.

Note Using the **clear access-list** command to delete the set of rules (**access-list** command statements) will also remove the **access-list** command statement used by NAT, so that any subsequent rules bound to an interface will not be processed until NAT has been reconfigured.

static Function

The **static** command must not be included in the certified PIX Firewall. The **static** command enables particular instances of NAT.

Saving Configuration

The **write memory** command should be used frequently when making changes to the configuration of the PIX Firewall. If the PIX Firewall reboots and resumes operation when uncommitted changes have been made, these changes will be lost and the PIX Firewall will revert to the last committed configuration.

Enabling Time-Stamp

By default, all audit records are not stamped with the time and date, which are generated from the system clock when an event occurs.

The certified PIX Firewall requires the Time-Stamp feature to be *enabled*. To enable the timestamp of audit events, use the **logging timestamp** command.

To ensure that the **timestamp** option remains the default, use the **write memory** command to save the option into the startup configuration.

Enabling Reliable Logging

By default, auditing events are transported to a remote syslog server over UDP. The certified PIX Firewall requires auditing events to be transported over TCP.

The TCP option is configured using the **logging host** *ip_address* **tcp**/*port_number* command.

With TCP logging configured, new sessions through the certified PIX Firewall will be disallowed if log messages cannot be forwarded to the remote host.

System Logs

System Log Messages for the Cisco Secure PIX Firewall Version 5.2 provides details on the PIX Firewall system logs.

The following sections are not supported on a certified PIX Firewall:

- Viewing Syslog Messages in a Telnet Console Session
- Receiving SNMP Requests
- Sending SNMP Traps
- Other Remote Management and Monitoring Tools

Release Notes Caveats

The following sections in the *Release Notes for the Cisco Secure PIX Firewall Version 5.2(1)* are not supported on a certified PIX Firewall:

- Cisco IOS Software Interoperability
- Cisco Secure VPN Client Interoperability
- Cisco VPN 3000 Concentrator and Client Interoperability
- PIX Firewall Manager Interoperability
- Failover Serial Connection
- AAA **access-list** Support
- Cisco VPN 3000 Client (Formerly the Altiga VPN Client)
- Failover Polling Time
- Important Notes:
  - AAA
  - Cisco Secure VPN Client
  - Cisco VPN 3000 Client and Concentrator
  - Failover

Related Documentation

Use this document in conjunction with the PIX Firewall documentation at the following site:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/index.htm

Cisco provides PIX Firewall technical tips at the following site:

http://www.cisco.com/warp/public/110/index.shtml#pix

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc., Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.